REMARKS/ARGUMENTS

1.)   Claim Amendments

The Applicant has amended claims 1-2, 6, 8, 13-14, 18, 23, and 30; claims 3-5, 7, 9-12, 15-17, 19-22, 26-29 and 31-33 have been canceled. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-2, 6, 8, 13-14, 18, 23-25, and 30 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.)   Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1-3, 5-14, 16-20 and 22-33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Reiche, *et al.* (U.S. Patent No. 6,092,196) in view of Niemi, *et al.* (RFC 3310, HTTP Digest Authentication Using AKA) and further in view of Inoue, *et al.* (U.S. Patent Publication No. 2006/0034238). The Applicant respectfully traverses the Examiner's rejection, but in order to expedite the allowance of the pending claims, the Applicant has further amended independent Claims 1 and 18 to recite additional limitations and to more clearly recite the novel and unobvious elements of the present invention. For example, certain limitations as previously recited in dependent Claims 9 and 32 have now been incorporated into independent Claim 1. A favorable reconsideration by the Examiner is therefore requested.

In rejecting Claim 18, the Examiner stated that Reiche disclosed the step of "sending to an authentication node, details of the request for access, said details including said temporary identity created by said remote server." Claim 18 has now been amended to recite the step of "<u>sending directly from said remote server to an authentication node in the UE's home network a second request for access</u>, said second request including said temporary identity created by said remote server and an identity of said remote server and instructing said authentication node to generate a challenge to said UE, said challenge including said temporary identity of the UE and said identity of said remote server." The Applicant respectfully submits that such recited step is not disclosed or taught by Reiche.

In Reiche, the Authentication Deamon (AD) does not directly sending a request for access to the authentication server. Instead, the AD returns a URL to the client browser instructing the client browser to redirect the request to the authentication server (Col. 9, lines 1-12). Accordingly, there is no direct request from the remote server to the authentication server in Niemi. Additionally, in Reiche, in response to a determination that a particular "browser" has never attempted to log on to it before, the authentication server then sends back a challenge to the client's browser to require the user to enter its authentication login information (Col. 9, col 15-25). Therefore, the "challenge" referenced in Reiche is a mere "pop up box" asking the user to enter its user id and password information (the browser will prompt the user for the authentication login information and the client will then see a dialog window on the screen that requests him to login). However, there is nothing in Reiche that discloses or teaches the step of a remote server directly sending a second request for access to the authentication server in the UE's home network wherein said second request instructing said authentication node to then generate a challenge to the UE <u>including the temporary identity of the UE and the identity of the remote server</u>. As further recited in dependent Claim 23, such a challenge is an HTTP Digest challenge rather than a mere pop-up box asking the user to enter its user id and password.

Moreover, nothing in Reiche discloses or teaches the step of the "<u>UE generating a password based on the challenge</u>, said password being associated with the temporary identity of the UE created by said remote server." Again, the only thing disclosed in Reiche is the authentication server prompting the <u>user to enter the login information</u> (Col 9, lines 15-35) with a new dialog box being displayed on the window. The login information is physically entered by the user and <u>no password is generated by the UE.</u> Furthermore, the login information entered by the user has nothing to do with the temporary identity of the UE as created by the remote server in accordance with the teachings of the present invention. As a result, there is nothing in Reiche that shows <u>the UE generating a password based on the challenge and wherein the password is associated with the temporary identity of the UE as created by the remote server.</u>

Lastly, nothing in Reiche discloses or teaches the step of "receiving at said remote server a first authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server." As further recited in now amended independent Claim 18, the purpose of such an authentication between the UE and the remote server is to allow "said remote server and said UE to challenge and authenticate a subsequent access request directly without sending said second request from said remote server to said authentication node". The Applicant respectfully submits that such novel and unobvious steps are not disclosed or taught by Reiche independently, or in combination with Niemi and/or Inoue.

The Examiner further stated that Niemi somehow disclosed generating a challenge including the temporary identity of the UE and the identity of the remote server. However, page 10, point 3 of Niemi merely shows a structure of a SIP register signal containing "username" and "realm" parameters. However, nothing in Niemi suggests that the username parameter as illustrated in this SIP register is a temporary identity for the UE as created by the remote server in response to receiving a request for access from the UE as presently claimed.

Lastly, the Inoue reference may disclose an authentication server residing within a home network. However, nothing in Inoue shows a remote server receiving a first request for access from a UE and then sending a second request directly from the remote server to the authentication server residing within the home network wherein said second request from the remote server containing the temporary identity for the UE as created by that remote server. Accordingly, Inoue independently, or in combination with the other cited references, still fails to anticipate or render obvious the presently pending independent Claim.

For at least the reasons as stated above, independent Claim 18 and its dependent claims are now in condition for allowance. Moreover, independent Claim 1, reciting similar limitations as set forth in Claim 18, and its dependent claims are likewise in condition for allowance. A favorable reconsideration by the Examiner is earnestly requested.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

/John C. Han,Reg#41403/

John C. Han
Registration No. 41,403

Date: November 17, 2010

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-7686
john.han@ericsson.com